94/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/848,670	05/04/2001	Shakeel Mustafa	SH0004	7787

7590 05/03/2006

SHAKEEL MUSTAFA
24831 Hendon St.
Laguna Hills, CA 92653

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/848,670	**Applicant(s)** MUSTAFA, SHAKEEL
	Examiner Courtney D. Fields	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 December 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 April 2005* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

2. This action is a **final rejection** and is intended to close the prosecution of this application. Applicant's reply under 37 CFR 1.113 to this action is limited either to an appeal to the Board of Patent Appeals and Interferences or to an amendment complying with the requirements set forth below.

If applicant should desire to appeal any rejection made by the examiner, a Notice of Appeal must be filed within the period for reply identifying the rejected claim or claims appealed. The Notice of Appeal must be accompanied by the required appeal fee of $500.00.

If applicant should desire to file an amendment, entry of a proposed amendment after final rejection cannot be made as a matter of right unless it merely cancels claims or complies with a formal requirement made earlier. Amendments touching the merits of the application which otherwise might not be proper may be admitted upon a showing a good and sufficient reasons why they are necessary and why they were not presented earlier.

A reply under 37 CFR 1.113 to a final rejection must include the appeal from, or cancellation of, each rejected claim. The filing of an amendment after final rejection, whether or not it is entered, does not stop the running of the statutory period for reply to the final rejection unless the examiner holds the claims to be in condition for allowance. Accordingly, if a Notice of Appeal has not been filed properly within the period for reply, or any extension of this period obtained under either 37 CFR 1.136(a) or (b), the application will become abandoned.

3. An examination of this application reveals that applicant is unfamiliar with patent prosecution procedure. While an inventor may prosecute the application, lack of skill in this field usually acts as a liability in affording the maximum protection for the invention disclosed. Applicant is advised to secure the services of a registered patent attorney or agent to prosecute the application, since the value of a patent is largely dependent upon skilled preparation and prosecution..The Office cannot aid in selecting an attorney or agent.

A listing of registered patent attorneys and agents is available on the USPTO Internet web site http://www.uspto.gov in the Site Index under “Attorney and Agent Roster.” Applicants may also obtain a list of registered patent attorneys and agents located in their area by writing to the Mail Stop OED, Director of the U. S. Patent and Trademark Office, PO Box 1450, Alexandria, VA 22313-1450

Specification

4. The disclosure is objected to because of the following informalities: The reference characters shown in Figure 11, (i.e., 430,435,505,510,535) are not taught in the specification. The reference character shown in Figure 9A, (i.e., 325) is not taught in the specification. The reference characters shown in Figure 9A, (i.e., 222,224,230, 300) have been added to the drawing, but are not taught in the specification. The reference character shown in Figure 9A, (i.e., 200) is taught in the specification, but not shown in the drawing. The reference characters shown in Figures 8A and 8B (i.e., 150,180,190) are not taught in the specification. The reference characters shown in Figure 5A and 5B, (i.e., 71;90) are not taught in the specification. As pointed out in previous office action, the above listed characters and additional characters found in Figures 13 and 14 (i.e., 820.825,830,840,883,887,889) are not mentioned in the description.

Appropriate correction is required.

5. The amendment filed 04 April 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Figure 9A introduces new reference characters 222,224,228, and the result D_{gkhv} which is not supported by the specification.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

6. Claims 1-3, 10 are objected to because of the following informalities: Each of these claims have incorrect punctuation marks in the body of the claim. For example in claim 1, there is a period behind the word versa, which is incorrect. A period should only follow at the end of the entire claim. For claim 2, a semicolon behind the number 1 is incorrect. The correct punctuation should be a comma. Similar objections are for the other dependent claims. Appropriate correction is required.

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). Original claims 1-22 were canceled. Once a claim has been canceled its original number is lost and every subsequent claim must be numbered in order of the last listed claim. Therefore, the claims need to be renumbered.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The number of rounds of encryption is determined

using either the information embedded in the random number or from the encrypted versions of the random number. This choice makes the claim vague and indefinite because if the choice for determining the number of rounds of encryption is based on the information embedded in the random number then steps (j) and (l) and (v) and (x) are not needed. With this choice, the host and the remote processors only need to mutual agree on specific locations of bits in the random number (information embedded in said random number) to determine the number of rounds for encryption/decryption. With the other choice, encrypted versions of the random number, a function from the first pool must be applied to the random number then a total number can be determined from the encrypted version of the random number. The two choices produce two distinct results on how to perform the encryption steps on the data segments, which in turn, makes the claim vague and indefinite. Claims 2-20 do not overcome the rationale give above and therefore are rejected due to their dependence on independent claim 1.

9. Claims 2-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Due to the cancellation and modification of the original dependent claims (See original claims), it is not clear as to what the actual metes and bounds are in applicant's invention.

***** As best understood by the Examiner of what the Applicant appears to claim in the invention, a rejection has been applied below.**

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1 and 21-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson et al. (US Patent No. 6,052,469).

Referring to the rejection of claim 1, Johnson et al. discloses a method for encryption and/or decryption data segments from a plurality of remote processors to a host processor or vice versa the method comprising the steps of at the host and the remote processors,

(a) mutually agreeing upon the locations of a pre-determined number of bits located within a random number of an arbitrary length through a set of pre-negotiated rules (See Column 8, lines 56-61 and Column 12, lines 19-30)

whereas the said random number constituting in a binary format segment (See Column 18, lines 5-17)

whereas an arbitrary length of random number means the size of the random number that can be processed by the system resources utilized in the participating remote and host processor (See Column 18, lines 5-10)

(b) defining at least two pools containing mathematical or logical functions of arbitrary complexity wherein:

(i) the first pool containing said functions that operate on random numbers (See Column 5, lines 62-67 and Column 18, lines 48-62)

(ii) the second pool containing said functions that operate on data segments that need to be encrypted (See Column 13, lines 17-30 and Column 18, lines 48-62)

(iii) the second pool containing inverse functions such that every function-defined in the second pool has an inverse function contained in it (See Column 20, lines 45-59)

(iv) the inverse functions for each of the functions contained in the second pool to be used in decrypting the data segments (See Column 20, lines 45-59)

whereas mathematical or logical functions of arbitrary complexity mean the functions that can be processed by the system resources utilized in the participating remote and host processor (See Column 13, lines 19-24)

(c) mutually agreeing upon the order of the functions defined in the first pool (See Column 13, lines 17-30)

(d) mutually agreeing upon the order of the functions defined in the second pool (See Column 13, lines 17-30)

(e) mutually agreeing upon establishing a unique relation between the functions defined in the first pool with the functions defined in the second pool for encrypting a data segment at the remote processor (See Column 18, lines 54-62)

(f) generating a random number in a binary format with the segment length containing at least one bit location mutually agreed upon between remote and host in accordance with step (a) (See Column 12, lines 39-49)

(g) identifying the specific locations of bits in the random number as mutually agreed upon between the said host and remote processors as indicated in step (a) (See Column 17, lines 42-55)

(h) calculating the numeric values of the bits al the said specific locations (See Column 14, lines 45-57)

(i) based on the result identifying the functions from the first pool and the second pool (See Column 18, lines 54-62)

(j) executing the functions as identified in the first pool to perform a round of encryption on the said random number (See Column 5, lines 62-67)

(k) executing the functions as identified in the second pool to perform a round of encryption on the said data segment (See Column 5, lines 62-67)

(l) replacing the encrypted random number as resulted in step (j) to be used in place of step (a) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(m) determining a number N that determines the total number of rounds of encryption from the information embedded in the said random number or in the encrypted versions of the random number (See Column 16, lines 46-58 and Column 17, lines 1-11)

(n) re-executing the procedure as described in steps (g) to (l) for N rounds of encryption (See Column 17, lines 1-11)

(o) transmitting the said encrypted segment to the host processor (See Column 17, lines 47-50)

(p) receiving the said encrypted data segment from the remote processor (See Column 17, lines 47-50)

(q) receiving the random number as generated by the remote processor in step (f) (See Column 12, lines 39-49)

(r) identifying the specific bits locations found within the said random number through the rules as mutually agreed upon in step (a) (See Column 14, lines 42-55)

(s) calculating the numeric values of the bits as found in the said specific locations (See Column 11, lines 20-40)

(t) based on the result of step (s), identifying functions set from the first pool (See Column 14, lines 45-57)

(u) based on the result of step (s) identifying the inverse functions set from the second pool (See Column 8, lines 11-40)

(v) executing the functions set as identified in the first pool to perform a first round of encryption on the said random number (See Column 12, lines 19-25)

(w) executing the identified inverse functions set as identified in step (u) to perform a round of decryption on the said data segment (See Column 8, lines 11-40)

(x) replacing the encrypted random number as resulted in step (v) in place of the random number as used in step (q) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(y) determining a number N that determines the total number of rounds of decryption from the information embedded in the said random number or in the encrypted versions of the random number (See Column 17, lines 1-11)

(z) re-executing the procedure as described in steps (q) to (x) for N rounds of decryption (See Column 8, lines 37-40, Column 16, lines 46-58)

(aa) and producing the decrypted data segment exactly to be the same as the original data segment before encryption (See Column 17, lines 1-11 and 47-50)

Referring to the rejection of claim 21 (**presently presented**), Johnson et al. discloses a method for encryption and/or decryption data segments from a plurality of remote processors to a host processor or vice versa the method comprising the steps of at the transmitting and receiving devices,

(a) defining a first set containing mathematical and/or logical functions (See Column 5, lines 62-67 and Column 18, lines 48-62)

(b) defining a second set containing inverse functions of every function defined in the first set as indicated in step (a) (See Column 20, lines 45-59)

(c) agreeing upon a set of rules to identify a single or plurality of specific bits locations present within a random number (See Column 8, lines 56-61 and Column 12, lines 19-30)

(d) sharing a random number long enough to contain a single or plurality of specific bits locations as mutually agreed upon in step (c) (See Column 18, lines 54-62)

wherein a random number constitutes a binary segment of arbitrary length (See Column 18, lines 5-10)

(e) agreeing upon the sequential order in which the functions defined in the first set are organized (See Column 13, lines 17-30)

(f) establishing one-to-one mapping between the functions defined in the first set with their corresponding inverse functions defined in the second set at the transmitting devices (See Column 20, lines 45-59)

(g) using information embedded within the random number to identify a function in the first set to (See Column 12, lines 39-49)

(h) encrypting the random number (See Column 5, lines 62-67)

(i) encrypted the data segment (See Column 17, lines 47-50)

(j) replacing the encrypted random number as resulted in step (h) to be used in place of step (g) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(k) determining a number N that determines the total number of rounds on said random number and the data segment (See Column 16, lines 46-58 and Column 17, lines 1-11)

(l) re-executing step (g) to (j) for N rounds of rounds at the receiving devices (See Column 17, lines 1-11)

(m) using the information embedded within the random number to identify a function in the first set to (See Column 17, lines 47-50)

(n) encrypting the random number (See Column 12, lines 39-49)

(o) identifying the inverse function from the second set that corresponds to the function used in the first set as identified in step (m) (See Column 14, lines 42-55)

(p) using the said inverse function from the second set to (See Column 8, lines 11-40)

(q) decrypting the received data segment (See Column 8, lines 11-40)

(r) replacing the encrypted random number resulted in step (n) to be used in place of step (m) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(s) determining a number N that determines the encryption rounds on the random number and the decryption rounds on the data segment (See Column 17, lines 1-11)

(t) re-executing steps (m) to step (r) for N number of rounds (See Column 8, lines 37-40, Column 16, lines 46-58)

(u) and producing the decrypted data segment exactly to be the same as the original data segment before encryption (See Column 17, lines 1-11 and 47-50)

Referring to the rejection of claim 22 (**presently presented**), Johnson et al. discloses a method for encryption and/or decryption data segments from a plurality of remote processors to a host processor or vice versa the method comprising the steps of at the host and the remote processors,

(a) defining a first set containing mathematical and/or logical functions (See Column 5, lines 62-67 and Column 18, lines 48-62)

(b) defining a second set containing mathematical and/or logical functions and their corresponding inverse functions (See Column 20, lines 45-59)

(c) sharing an identical password constituting a binary segment of arbitrary length (See Column 18, lines 5-10)

(d) using the information embedded in the said password identifying a function contained in the first set (See Column 13, lines 17-30)

(e) populating the first column of a table by entering the functions as identified from the first set in step (d) as the ith function entry into the said table (See Column 20, lines 45-59)

(f) encrypting the password with the function as identified in step (e) (See Column 5, lines 62-67)

(g) using information embedded in the password to identify a function contained in the second set (See Column 12, lines 39-49)

(h) populating the second column of a table by entering the functions as identified from the second set in step (g) as the jth function entry into the said table (See Column 20, lines 45-59)

(i) populating the third column of a table by entering the functions as identified from the third set in step (g) as the jth inverse function entry into the said table (See Column 20, lines 45-59)

(j) replacing the encrypted password as resulted in step (f) to be used in place of step (c) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(k) determining a number N that determines the total number of entries in the first, second, and third columns of the said table (See Column 16, lines 46-58 and Column 17, lines 1-11)

(l) re-executing step (c) to (j) for N rounds of rounds at the remote processor (See Column 17, lines 1-11)

(m) determining a number E which determines the number of encryption rounds to be performed on a data segment such that 1<E<N (See Column 17, lines 47-50)

(n) encrypting a data segment by using the functions as listed under the second column with the ith function entry being vary from 1 to E number of encryption rounds (See Column 12, lines 39-49)

(o) transmitting the encrypted data segment produced by the step (n) to the host processor (See Column 12, lines 39-49)

(p) receiving the encrypted data segment resulting from step (o) (See Column 16, lines 46-58 and Column 17, lines 47-50)

(q) determining a number D which determines the number of decryption rounds to be performed on the received encrypted data segment such that D=E (See Column 17, lines 1-11)

(r) decrypting the said data segment by using the inverse functions as listed under the third column with the ith function entry varying being vary from 1 to D number of decryption rounds (See Column 8, lines 11-40)

(s) and producing the decrypted data segment exactly to be the same as the original data segment before encryption (See Column 17, lines 1-11 and 47-50)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
April 26, 2006

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137